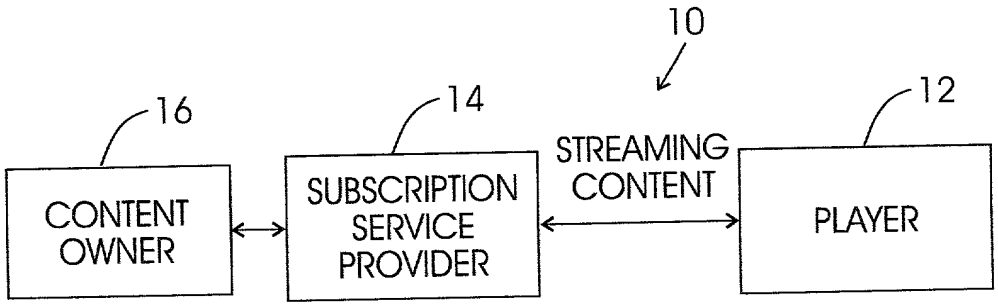


FIG. 1

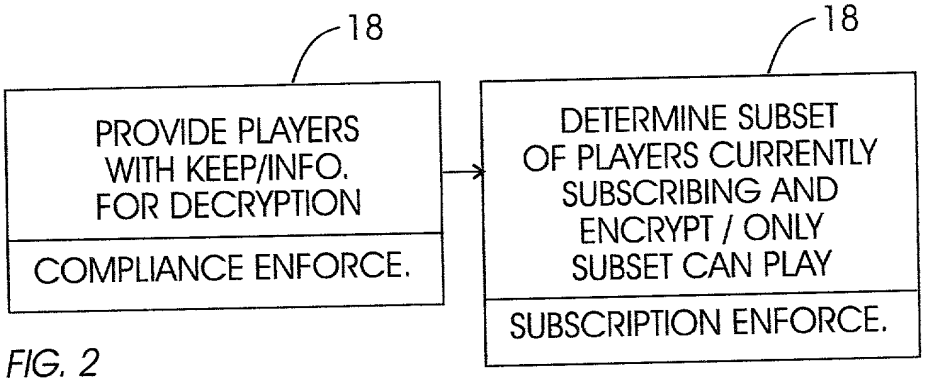


FIG. 2

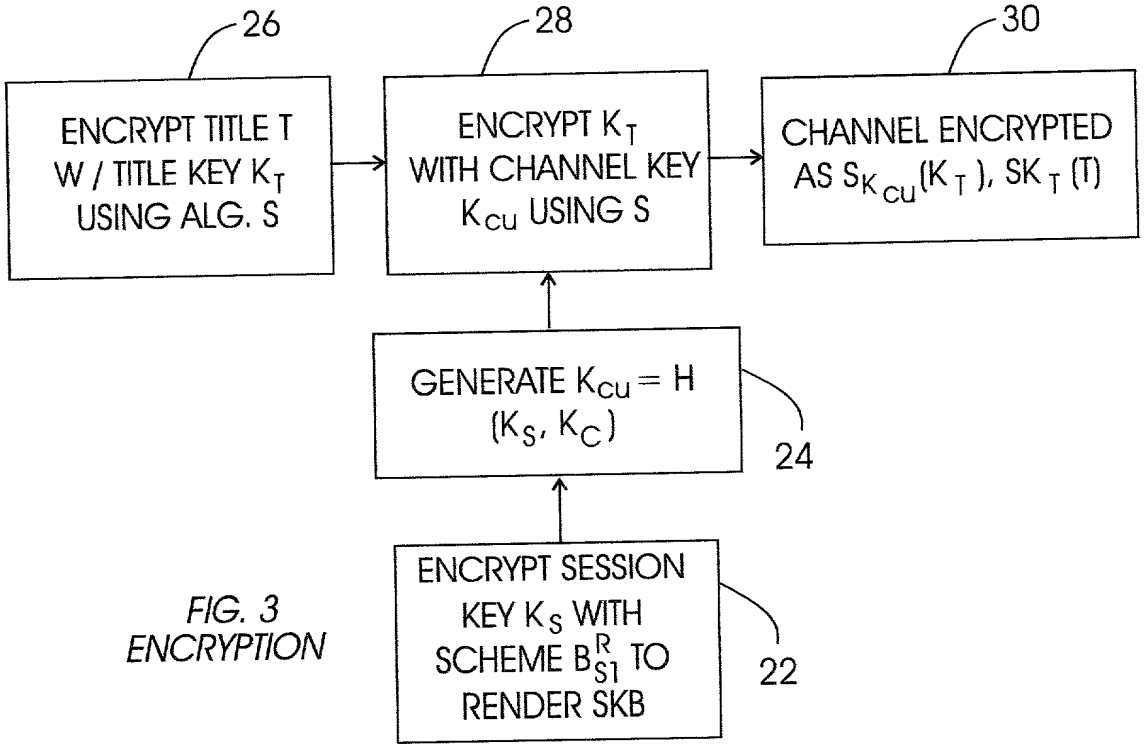


FIG. 3
ENCRYPTION

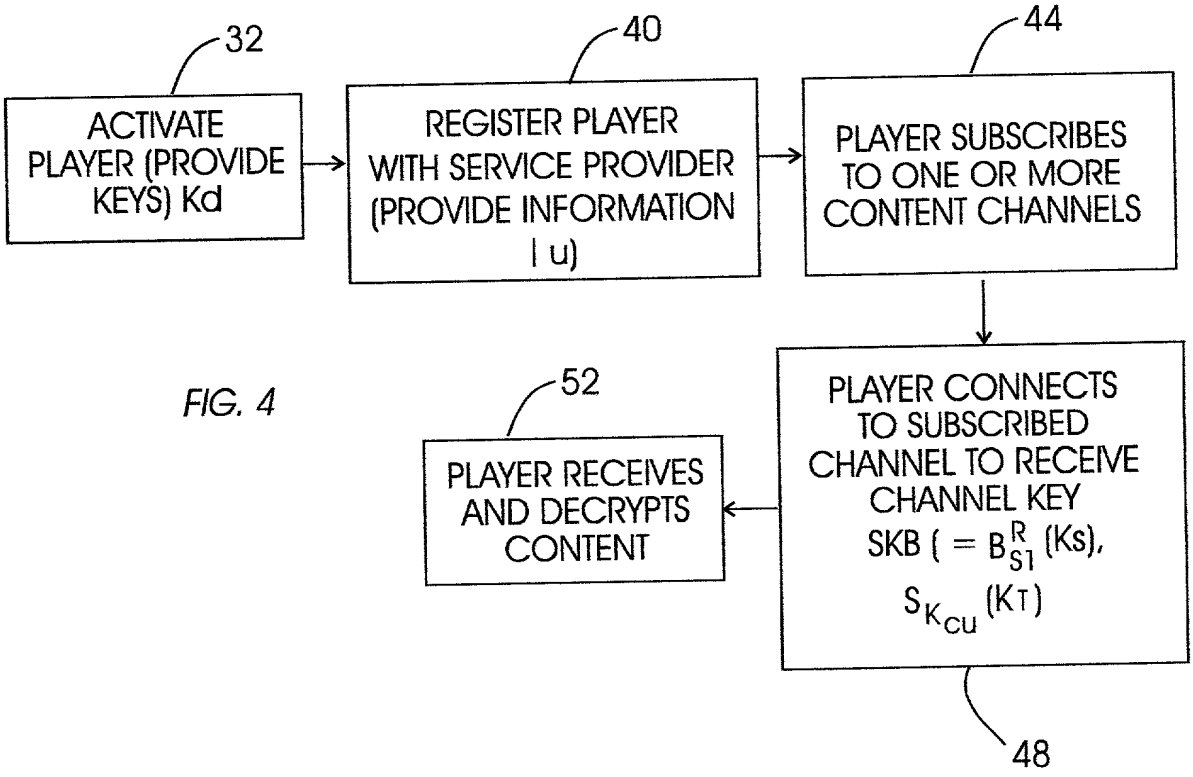
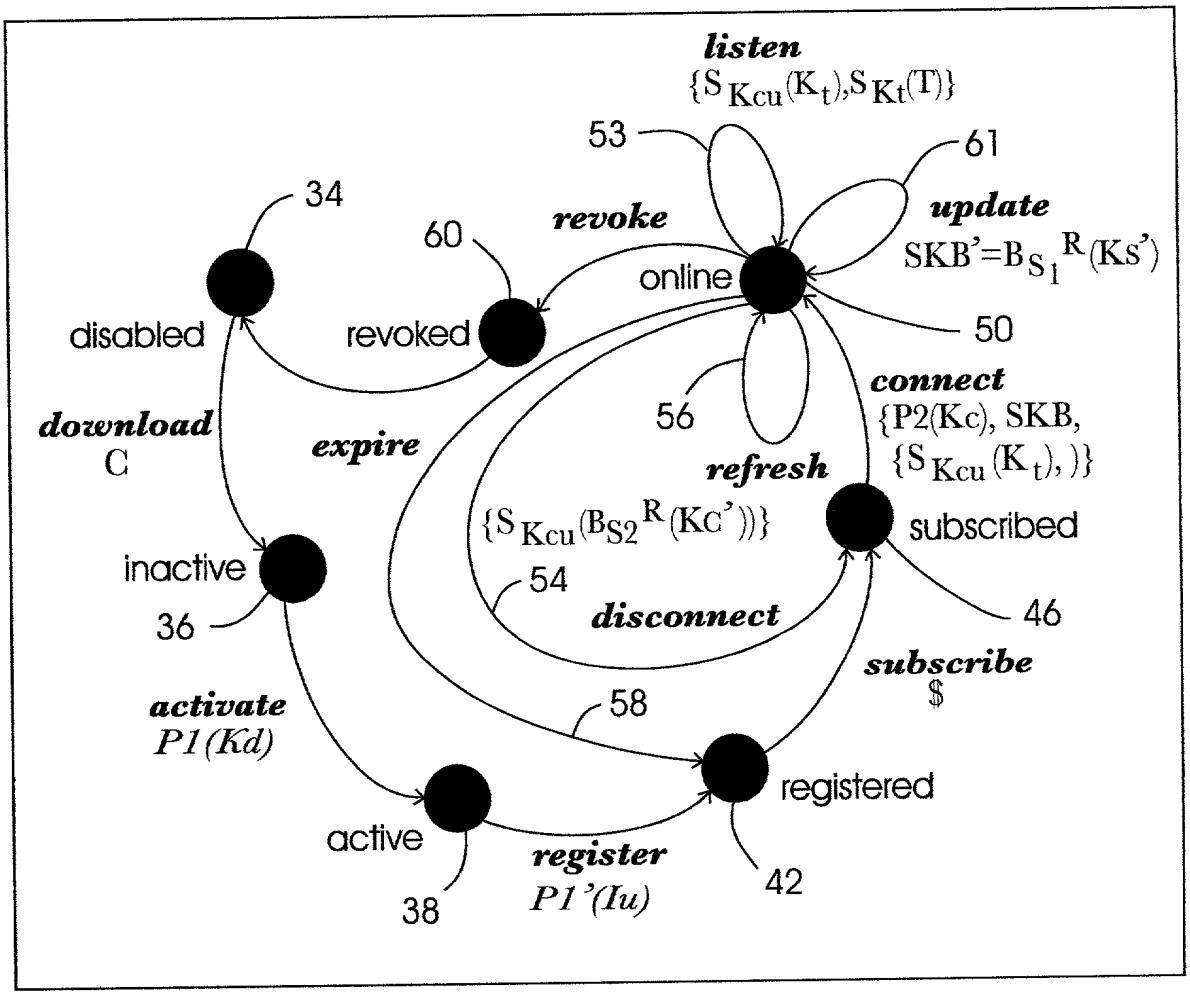

32
ACTIVATE PLAYER (PROVIDE KEYS) Kd
40
REGISTER PLAYER WITH SERVICE PROVIDER (PROVIDE INFORMATION | u)
44
PLAYER SUBSCRIBES TO ONE OR MORE CONTENT CHANNELS
PLAYER CONNECTS TO SUBSCRIBED CHANNEL TO RECEIVE CHANNEL KEY
SKB (= B_{S1}^{R} (Ks),
$S_{K_{CU}}$ (KT)
48
52
PLAYER RECEIVES AND DECRYPTS CONTENT

FIG. 4



C - Code
T - Title

$ - Financial transaction

K_d - Device Keys
Iu - User info
K_s - Session key
K_c - Channel key
K_{cu} - Channel unique key
K_t - Title key
SKB - Session key block

Encryption	Point to point	Multicast
Symmetric		**S**
Subset cover difference		$\mathbf{B}_{S1}{}^{R}$, $\mathbf{B}_{S2}{}^{R}$
Public key	*P1, P1', P2*	

FIG. 5